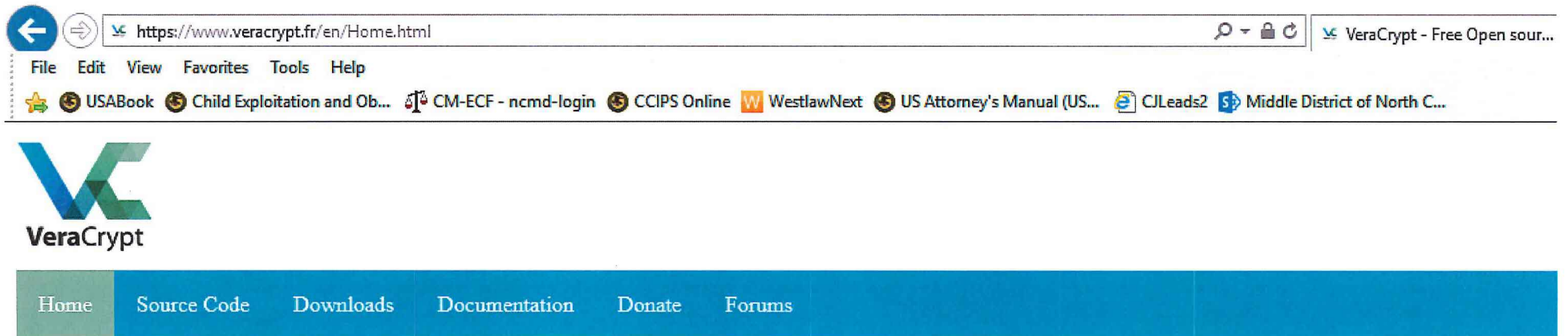


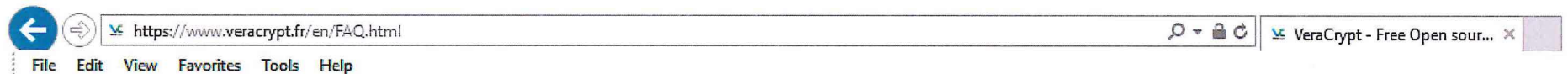
ATTACHMENT A

Graphic 1:



VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. Brought to you by **IDRIX** (<https://www.idrix.fr>) and based on TrueCrypt 7.1a.

Graphic 2:



What's the difference between TrueCrypt and VeraCrypt?

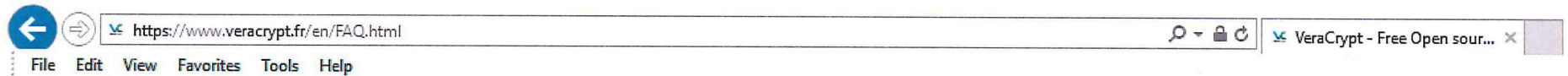
VeraCrypt adds enhanced security to the algorithms used for system and partitions encryption making it immune to new developments in brute-force attacks.

It also solves many vulnerabilities and security issues found in TrueCrypt.

As an example, when the system partition is encrypted, TrueCrypt uses PBKDF2-RIPEMD160 with 1000 iterations whereas in VeraCrypt we use 327661. And for standard containers and other partitions, TrueCrypt uses at most 2000 iterations but VeraCrypt uses 655331 for RIPEMD160 and 500000 iterations for SHA-2 and Whirlpool.

This enhanced security adds some delay only to the opening of encrypted partitions without any performance impact to the application use phase. This is acceptable to the legitimate owner but it makes it much harder for an attacker to gain access to the encrypted data.

Graphic 3:



I forgot my password – is there any way ('backdoor') to recover the files from my VeraCrypt volume?

We have not implemented any 'backdoor' in VeraCrypt (and will never implement any even if asked to do so by a government agency), because it would defeat the purpose of the software. VeraCrypt does not allow decryption of data without knowing the correct password or key. We cannot recover your data because we do not know and cannot determine the password you chose or the key you generated using VeraCrypt. The only way to recover your files is to try to "crack" the password or the key, but it could take thousands or millions of years (depending on the length and quality of the password or keyfiles, on the software/hardware performance, algorithms, and other factors). Back in 2010, there was news about the [FBI failing to decrypt a TrueCrypt volume after a year of trying](#). While we can't verify if this is true or just a "psy-op" stunt, in VeraCrypt we have increased the security of the key derivation to a level where any brute-force of the password is virtually impossible, provided that all security requirements are respected.

Graphic 4:

